UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,644	10/15/2003	Steven L. Teixeira	VIV/0012.01	2643

28653 7590 04/14/2010

JOHN A. SMART
201 LOS GATOS
SARATOGA RD, #161
LOS GATOS, CA 95030-5308

EXAMINER	
BARRON JR, GILBERTO	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/14/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte STEVEN L. TEIXEIRA

Appeal 2009-004088
Application 10/605,644[1]
Technology Center 2400

Decided: April 14, 2010

Before JAMES D. THOMAS, HOWARD B. BLANKENSHIP, and JAMES R. HUGHES, *Administrative Patent Judges.*

HUGHES, *Administrative Patent Judge.*

DECISION ON APPEAL

---

[1] Application filed October 15, 2003. The real party in interest is Check Point Software Technologies., Inc. (Br. 3.)

STATEMENT OF THE CASE

The Appellant appeals from the Examiner's rejection of claims 1-55 under authority of 35 U.S.C. § 134(a). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellant's Invention

Appellant invented a computer system and method for securing sensitive user information. The system receives a user's sensitive information, computes a "data shadow" of the user's sensitive information, stores the data shadow, discards the user's sensitive information, detects any attempted transmission of the user's sensitive information utilizing the data shadow, and blocks the unauthorized attempted transmission of the user's sensitive information. (Spec. ¶¶ [0007], [0014].)[2]

Representative Claim

Independent claim 1 further illustrates the invention. It reads as follows:

> 1. In a computer system, a method for protecting sensitive information, the method comprising:
>
> receiving input of sensitive information from a user;
>
> computing a data shadow of the sensitive information for storage in a repository, and thereafter discarding the input so that the sensitive information itself is not stored;

[2] We refer to Appellant's Specification ("Spec.") and Appeal Brief ("Br.") filed November 13, 2007. We also refer to the Examiner's Answer ("Ans.") mailed January 23, 2008.

based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and

blocking any detected attempt to transmit the sensitive information that is not authorized by the user.

References

The Examiner relies on the following reference as evidence of unpatentability:

Margolus US 2004/0162808 A1 Aug. 19, 2004
(filed Jan. 7, 2004)
(Divisional of Appl. No. 09/785,535 filed Feb. 16, 2001)

Rejections on Appeal

The Examiner rejects claims 1-55 under 35 U.S.C. § 102(e) as being anticipated by Margolus.

ISSUE

Based on Appellant's contentions, as well as the findings and conclusions of the Examiner, the pivotal issue before us is as follows.

Does the Examiner err in finding the Margolus reference discloses: (1) discarding user sensitive information so that it is not stored in the system; and (2) blocking unauthorized transmission of the user sensitive information?

FINDINGS OF FACT (FF)

Appellant's Specification

1. Appellant's Specification describes computing a "data shadow" from user sensitive information – a data structure element that may include a regular expression (format information for the user sensitive information) and a hash of the user sensitive information (for example, an MD-5 hash), i.e., a "fingerprint" of the user sensitive information – but the user sensitive information itself is not stored and is discarded after the data shadow is computed. (¶¶ [0042]-[0048], [0078].) Appellant's Specification also describes detecting and blocking unauthorized transmission of the user sensitive information utilizing the data shadow. (¶¶ [0063], [0085].)

Margolus Reference

2. Margolus describes a computer data repository (data storage system) and method that stores data to locations associated with a digital "fingerprint" or "dataname." Margolus receives a user data item, encrypts the data item, creates a dataname (digital fingerprint) for the data item, and stores the data item and the dataname in the system. (¶¶ [0010]-[0011], [0058]-[0060].)

3. Margolus also describes determining whether a data item is already stored in the system utilizing a comparison of datanames. (¶¶ [0011], [0012], [0060].)

PRINCIPLES OF LAW

Burden on Appeal

The allocation of burden requires that the United States Patent and Trademark Office (USPTO) produce the factual basis for any rejection in order to provide an applicant with notice of the reasons why the applicant is not entitled to a patent on the claim scope sought. *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992); *In re Piasecki*, 745 F.2d 1468, 1472 (Fed. Cir. 1984); *Ex Parte Frye*, No. 2009-006013, 2010 WL 889747, *3 (BPAI) (Precedential). An appellant has the opportunity on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn,* 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998), *overruled in part on other grounds*, *KSR*, 550 U.S. at 422); *Ex Parte Frye*, 2010 WL 889747 at *4.

Anticipation

Anticipation is a question of fact. *In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997). Under 35 U.S.C. § 102, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987) (citations omitted); *see also Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005)(citation omitted).

ANALYSIS

Appellant contends that the disclosed "improved lockbox approach (which expressly eschews storage of the data item itself) is not taught or suggested by Margolus' network storage solution, which clearly stores at least one copy of the data item of interest, as it is in fact a network storage system." "Margolus teaches, if anything in this regard, away from Appellant's claimed approach." (Br. 11.) Appellant also contends that "Margolus provides no teaching or suggestion that would suggest his system may detect and trap outbound transmission of sensitive user information, all without ever storing a copy of the user information itself." (Br. 9.) In summary, Appellant contends that Margolus fails to disclose (and actually teaches away from): (1) discarding user sensitive information so that it is not stored in the system; and (2) blocking unauthorized transmission of the user sensitive information. The Examiner, on the other hand, finds that the Margolus reference discloses each feature of Appellant's claim 1 and maintains that the claim is properly rejected. (Ans. 3, 12.) Accordingly, we decide the question of whether Margolus discloses discarding user sensitive information so that it is not stored, and blocking unauthorized transmission of the user sensitive information.

After reviewing the record on appeal, we agree with Appellant, and we find the Margolus reference does not disclose discarding (and/or not storing) user sensitive information, as well as blocking unauthorized transmission of the user sensitive information. We broadly, but reasonably construe the disputed limitations of Appellant's claim 1, in view of Appellant's Specification disclosure, to compute a "data shadow" or "fingerprint" from received user sensitive information such that the user

sensitive information itself is not stored and is discarded after the data shadow is computed; and also to detect and block unauthorized transmission of the user sensitive information utilizing the data shadow. (FF 1.)

The Margolus reference describes receiving a user data item, encrypting the user data item, computing a dataname (fingerprint) for the user data item, and determining whether a particular user data item is already stored in the system by utilizing a comparison of datanames. (FF 2-3.) Thus we find that Margolus teaches several features of Appellant's system/method, including receiving a user data item, computing a fingerprint for the user data item, and detecting a particular user data item using the fingerprint. However, Margolus also describes storing the user data item and the dataname in its repository. (FF 2.) There is simply no explicit or inherent disclosure in Margolus of discarding (and not storing) user sensitive information, nor blocking transmission of user sensitive information. Thus, we are constrained by the record before us, and find that Margolus does not disclose discarding, not storing, and blocking user sensitive information. Accordingly, we reverse the Examiner's anticipation rejection of independent claim 1 and its dependent claims 2-32.

Appellant's independent claim 33 includes limitations of similar scope directed to discarding and trapping user sensitive information. We, therefore, reverse the Examiner's anticipation rejection of independent claim 33 and its dependent claims 34-46 for the reasons set forth with respect to claim 1, *supra*.

Appellant's independent claim 47, while slightly different in scope, also includes limitations directed to not saving and detecting outgoing transmission of user sensitive information. For the reasons set forth

previously with respect to claim 1, we find that Margolus also does not disclose these limitations. Accordingly, we reverse the Examiner's anticipation rejection of independent claim 47 and its dependent claims 48-55.

CONCLUSION OF LAW

On the record before us, we find that Appellant has established that the Examiner erred in finding the Margolus reference discloses discarding user sensitive information so that it is not stored in the system, and blocking unauthorized transmission of the user sensitive information.

DECISION

We reverse the Examiner's rejection of claims 1-55 under 35 U.S.C. § 102(e).

REVERSED

erc

John A. Smart
201 Los Gatos Saratoga Rd., #161
Los Gatos, CA 95030-5308